

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 01-217689

(43)Date of publication of application : 31.08.1989

(51)Int.Cl.

G06K 19/00
B42D 15/02

(21)Application number : 63-043461

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 26.02.1988

(72)Inventor : IJIMA YASUO

(54) PORTABLE ELECTRONIC EQUIPMENT

(57)Abstract:

PURPOSE: To diversify a method for establishing the security of an IC card system by registering plural cumulative upper limit values referred at the time of the discord of the collation of a password number and selecting the cumulative upper limit based on a corresponding relation determined in the IC card.

CONSTITUTION: The plural cumulative upper limit values referred at the time of the discord of the collation of the password number are registered, for instance, to select the cumulative upper limit value based on the corresponding relation determined in a main device. Accordingly, the referred cumulative upper limit values are not commonly used to the plural password numbers to establish the difference of the security level of the password number itself. Thereby, the method for establishing the security of the IC card system can be diversified.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C) 1998,2000 Japan Patent Office

⑨ 日本国特許庁(JP)

⑩ 特許出願公開

⑫ 公開特許公報(A)

平1-217689

⑤ Int. Cl.⁴

G 06 K 19/00
B 42 D 15/02
G 06 K 19/00

識別記号

3 3 1

庁内整理番号

P-6711-5B
J-8302-2C
R-6711-5B

④ 公開 平成1年(1989)8月31日

審査請求 未請求 請求項の数 1 (全11頁)

⑭ 発明の名称 携帯可能電子装置

⑯ 特 願 昭63-43461

⑰ 出 願 昭63(1988)2月26日

⑱ 発 明 者 飯 島 康 雄 神奈川県川崎市幸区柳町70番地 株式会社東芝柳町工場内
⑲ 出 願 人 株 式 会 社 東 芝 神奈川県川崎市幸区堀川町72番地
⑳ 代 理 人 弁 理 士 鈴 江 武 彦 外 2 名

明 細 書

1. 発明の名称

携帯可能電子装置

2. 特許請求の範囲

メモリ部と、このメモリ部に対してデータの読出しおよび書込みを行なうための制御部を有し、選択的に外部からの入出力を行なう手段を具備する携帯可能電子装置であって、

前記メモリ部に記憶されている複数の第1のデータ列と、

外部から入力された第2のデータ列と前記メモリ部に記憶されている前記複数の第1のデータ列のうち選択的に1つの第1のデータ列とを両者の間に所定の関係があるか否かを照合する照合手段と、

この照合手段の照合結果が否定的であった際その否定回数を累積する累積手段と、

複数の累積上限値を記憶する記憶手段と、

この記憶手段から前記累積手段で累積された回数と比較するための1つの累積上限値を選択する選択手段と、

この選択手段で選択された累積上限値と前記累積手段で累積された回数とを比較する比較手段と、

この比較手段の比較結果に基づき前記複数の第1のデータ列のうち選択された第1のデータ列の使用を禁止する禁止手段と

を具備したことを特徴とする携帯可能電子装置。

3. 発明の詳細な説明

〔発明の目的〕

(産業上の利用分野)

本発明は、たとえばクレジットカードやキャッシュカードなどとして用いられる、いわゆるICカードと称される携帯可能電子装置に関する。

(従来の技術)

近年、クレジットカードやキャッシュカードなどの磁気ストライプ付カード、いわゆる磁気カードが普及している中、これらに代わって新たに記憶容量を拡大した、消去可能な不揮発性メモリおよび、これらを制御するCPUなどの制御素子を有するICチップを内蔵した、いわゆるICカードが注目されている。

このようなICカードが運用されるシステムとして、最近では複数のアプリケーションを1つのICカードで利用する動きがある。ICカードの利用時には、本人確認を行なうために暗証番号の照合を行なうようになっている。

すなわち、あらかじめICカードのメモリ内に暗証番号を登録しておき、外部装置にて暗証番号を入力することにより、この入力された暗証番号と登録された暗証番号との照合をカード内部で行なう。そして、この照合結果に基づき、以降のオペレーションの可否をカード自身で判断することにより、メモリ内のデータのセキュリティ保持を実現している。また、照合不一致の際には、不一致回数をカード内で累積し、あらかじめメモリ内に登録されている累積上限値(リミット値)との比較を行ない、累積回数がその累積上限値に達すると、以降その暗証番号が使用不可能となるよう制御している。

さて、先に述べたようにシステムが複雑化するにつれ、ICカードに登録される暗証番号の数も

多くなり、その運用セキュリティレベルもそれぞれ異なる。しかるに、累積上限値が複数の暗証番号の全てに対して共通に用いられると、この運用セキュリティレベルの差が実現しにくくなる。

(発明が解決しようとする課題)

本発明は、上記したように暗証番号の照合不一致時に参照する累積上限値が複数の暗証番号に対して共通に使用されると、暗証番号自身のセキュリティレベルの格差を確立できなくなるという問題点を解決すべくなされたもので、暗証番号の照合不一致時に参照する累積上限値が複数の暗証番号に対して共通に使用されなくなり、暗証番号自身のセキュリティレベルの格差を確立できる携帯可能電子装置を提供することを目的とする。

[発明の構成]

(課題を解決するための手段)

本発明は、メモリ部と、このメモリ部に対してデータの読出しおよび書込みを行なうための制御部を有し、選択的に外部からの入出力を行なう手段を具備する携帯可能電子装置であって、前記

メモリ部に記憶されている複数の第1のデータ列(たとえば暗証番号)と、外部から入力された第2のデータ列(たとえば暗証番号)と前記メモリ部に記憶されている前記複数の第1のデータ列のうち選択的に1つの第1のデータ列とを両者の間に所定の関係があるか否かを照合する照合手段と、この照合手段の照合結果が否定的であった際その否定回数を累積する累積手段と、複数の累積上限値を記憶する記憶手段と、この記憶手段から前記累積手段で累積された回数と比較するための1つの累積上限値を選択する選択手段と、この選択手段で選択された累積上限値と前記累積手段で累積された回数とを比較する比較手段と、この比較手段の比較結果に基づき前記複数の第1のデータ列のうち選択された第1のデータ列の使用を禁止する禁止手段とを具備している。

(作用)

たとえば暗証番号の照合不一致時に参照する累積上限値を複数登録しておき、本装置内で定められた対応関係に基づき累積上限値を選択するこ

とにより、参照する累積上限値が複数の暗証番号に対して共通に使用されなくなり、暗証番号自身のセキュリティレベルの格差を確立できる。これにより、たとえばICカードシステムのセキュリティ性確立方法が多様化する。

(実施例)

以下、本発明の一実施例について図面を参照して説明する。

第20図は本発明に係る携帯可能電子装置としてのICカードを取扱う端末装置の構成例を示すものである。すなわち、この端末装置は、ICカード1をカードリーダー・ライタ2を介してCPUなどからなる制御部3と接続可能にするとともに、制御部3にキーボード4、CRTディスプレイ装置5、プリンタ6およびフロッピーディスク装置7を接続して構成される。

ICカード1は、ユーザが保持し、たとえば商品購入などの際にユーザのみが知得している暗証番号の参照や必要データの蓄積などを行なうもので、たとえば第18図にその機能ブロックを示す

ように、リード・ライト部11、暗証設定・暗証照合部12、および暗号化・復号化部13などの基本機能を実行する部分と、これらの基本機能を管理するスーパーバイザ14とで構成されている。リード・ライト部11は、データメモリなどに対してデータの読出し、書込み、あるいは消去を行なう機能である。暗証設定・暗証照合部12は、ユーザが設定した暗証番号の記憶および読出禁止処理を行なうとともに、暗証番号の設定後にその暗証番号の照合を行ない、以後の処理の許可を与える機能である。暗号化・復号化部13は、たとえば通信回線を通じて制御部3から他の端末装置へデータを送信する場合の通信データの漏洩、偽造を防止するための暗号化や暗号化されたデータの復号化を行なうものであり、たとえばDES (Data Encryption Standard) など、十分な暗号強度を有する暗号化アルゴリズムにしたがってデータ処理を行なう機能である。スーパーバイザ14は、カードリーダー・ライタ2から入力された機能コードもしくはデータの付加された機能コードを

解釈し、前記基本機能のうち必要な機能を選択して実行させる機能である。

これらの諸機能を実現させるために、ICカード1は、たとえば第17図に示すように、CPUなどの制御素子(制御部)15、データメモリ(メモリ部)16、プログラムメモリ17、およびカードリーダー・ライタ2との電気的接触を得るためのコンタクト部18によって構成されており、これらのうち制御素子15、データメモリ16、およびプログラムメモリ17は1つのICチップ(あるいは複数のICチップ)で構成されてICカード本体内に埋設されている。プログラムメモリ17は、たとえばマスクROMで構成されており、前記各基本機能を実現するサブルーチンを編めた制御素子15の制御プログラムなどを記憶するものである。データメモリ16は、各種データの記憶に使用され、たとえばEEPROMなどの消去可能な不揮発性メモリで構成されている。

カードリーダー・ライタ2は、ICカード1と制御部3との間で機能コードやデータの授受を行な

うものであり、制御部3からのマクロ命令に基づいてICカード1に対して1命令1応答動作を行なう機能をも有している。具体的には、たとえば第19図に示すように、図示しないカード挿入口に挿入されたICカード1を所定の位置まで搬送する搬送機構21、所定の位置にセットされたICカード1のコンタクト部18に電気的に接触されるコンタクト部22、全体の制御を司るCPUなどからなる制御部23、制御部23と制御部3との間で命令データや応答データの授受を行なうための入出力インタフェース回路24、およびデータを記憶するデータメモリ25などから構成されている。

前記データメモリ16は、たとえば第3図に示すように、エリア定義テーブル161、暗証情報テーブル162、およびデータエリア163に大別されており、特にエリア定義テーブル161には、暗証情報エリア定義テーブル164およびトランザクションデータエリア定義テーブル165を含んでいる。

暗証情報エリア定義テーブル164は、データエリア163内に暗証情報エリアを定義する定義情報が格納されており、この定義情報は、たとえば第4図に示すように、エリア番号、エリア先頭アドレス、およびエリアサイズからなる一連のデータ列の集合体である。

トランザクションデータエリア定義テーブル165は、データエリア163内にトランザクションデータエリアを定義する定義情報が格納されており、この定義情報は、たとえば第5図に示すように、エリア番号、エリア先頭アドレス、エリアサイズ、およびアクセス条件情報からなる一連のデータ列の集合体である。

データエリア163は、暗証情報エリア定義テーブル164およびトランザクションデータエリア定義テーブル165によってエリア定義され、種々のデータが格納されるもので、その具体例を第6図に示す。

暗証情報テーブル162は、たとえば第7図に示すように、インデックス部、暗証番号エリアの

エリア番号部、エラーカウンタエリアのエリア番号部、エラーリミットエリアのエリア番号部、および暗証照合状態エリアのエリア番号部からなる一連のデータ列の集合体である。

インデックス部は、後述する暗証照合命令データ（第2図参照）中のインデックス指定情報と関連付けられて動作するようになっている。すなわち、暗証照合命令データ中のインデックス指定情報と同一のインデックスを捜し、見付ければ、それに対応する暗証番号などが照合の対象となるのである。

暗証番号エリアのエリア番号部は、照合対象として指定された暗証番号が格納されているデータエリア163内の暗証番号エリアのエリア番号である。

エラーカウンタエリアのエリア番号部は、制御素子15内のRAM上にある第1のエラーカウンタ（第8図参照）を指定するとともに、データエリア163内の第2のエラーカウンタエリアのエリア番号となっている。

よびエリアサイズ「10バイト」より、第6図に示すデータエリア163を参照し、暗証番号「11111111」を得る。ここで、暗証番号エリアは、1バイトの暗証番号のバイト数を示すレンジ部と可変長の暗証番号部からなっている。レンジ部が「FF」Hexのときは暗証番号が格納されていないと認識する。

次に、対応するエラーカウンタエリアのエリア番号は、第7図により「11」となっているので、同様にしてエリア先頭アドレスTA₁およびエリアサイズ「1バイト」より、第6図に示すデータエリア163を参照し、第2のエラーカウンタの値「00」を得る。

同様な方法で、インデックス「31」によって指定された暗証番号は8バイトデータで「11111111」という値、また第2のエラーカウンタの値は「00」、エラーリミット値は第1のエラーカウンタとして「3」、第2のエラーカウンタとして「5」であり、照合状態ビットは第10図の0ビット目に対応することをICカ

エラーリミットエリアのエリア番号部は、第1および第2のエラーカウンタのリミット値（累積上限値）が格納されているデータエリア163内のエラーリミットエリアのエリア番号である。なお、このエラーリミットエリアは1バイトエリアであり、たとえば第9図にそのフォーマットを示すように、上位4ビットで第1のエラーカウンタのリミット値を示し、下位4ビットで第2のエラーカウンタのリミット値を示す。

暗証照合状態エリアのエリア番号部は、制御素子15内のRAM上にある照合状態ビット（第10図参照）のどのビットを照合状態フラグとするかを識別する情報が格納されているデータエリア163内の暗証照合状態エリアのエリア番号である。

たとえばインデックス「31」を指定すると、これに対応する暗証番号エリアのエリア番号は第7図により「01」である。これを第4図に示す暗証情報エリア定義テーブル164から検索し、対応するエリア先頭アドレス「TA₀」お

ード1の制御素子15が認識するようになっている。

次に、このような構成において動作を説明する。まず、カードリーダー・ライタ2は、第11図に示すフローチャートにしたがって動作する。すなわち、定常状態においては、制御部3からの命令データ待ち状態となっている。この状態において、制御部3から命令データが入力されると、制御部23は、ICカード1が実行中であるか否かを判断し、実行中である場合には多重命令データエラーを意味する応答データを制御部3に出力し、命令データ待ち状態に戻る。ICカード1が実行中でない場合には、制御部23は、ICカード1に命令データを出力し、ICカード1からの応答データ待ち状態となる。ICカード1からの応答データがあると、制御部23は、命令がマクロ命令である場合には再びICカード1に命令データを出力し、そうでない場合には制御部3に応答データを出力し、命令データ待ち状態に戻る。

なお、カードリーダー・ライタ2からICカード

1に出力される命令データは、たとえば第12図に示すようなフォーマットであり、同図(a)に示すように機能コードのみの形態、または同図(b)に示すように機能コードにデータを付加した形態がある。

ICカード1は、第13図に示すフローチャートにしたがって動作する。すなわち、定常状態においては、カードリーダー・ライター2からの命令データ待ち状態となっている。この状態において、カードリーダー・ライター2から命令データが入力されると、制御素子15は、その命令データにしたがって基本機能を実行し、カードリーダー・ライター2にその処理結果を示す応答データを出力し、命令データ待ち状態に戻る。

この場合の応答データは、たとえば第14図に示すようなフォーマットであり、処理結果を示す情報に入力された命令データに含まれた機能コードを付加し、カードリーダー・ライター2との間のシーケンスが乱れた場合の防護措置を講じておく。

次に、暗証番号の照合動作について第1図に示

ならば、制御素子15は、そのインデックスに対応する暗証番号エリアを参照する。ここで、もし暗証番号エリアのレンジ部が“FF”Hexとなっていれば、制御素子15は、暗証番号が格納されていないと認識し、暗証番号未設定を意味する応答データを出力し、命令データ待ち状態に戻る。

もし、暗証番号エリアのレンジ部が“FF”Hex以外であれば、制御素子15は、暗証番号が格納されているものと認識し、次に対応する第2のエラーカウンタの値およびそのリミット値を読出し、両者の比較照合を行なう。この比較照合の結果、もしリミット値が第2のエラーカウンタの値よりも大きければ、制御素子15は、暗証番号の照合処理を行なう。上記比較照合の結果、もしリミット値が第2のエラーカウンタの値よりも大きくなければ、制御素子15は、インデックスに対応する暗証照合状態エリアを参照し、そのエリアの内容を読出すことにより、対応する照合状態ビットを「0」にし、暗証番号使用不可を意味

すフローチャートを参照して説明する。命令データが入力されると、制御素子15は、その命令データが例えば第2図に示すようなフォーマットを持つ暗証照合命令データであるか否かを判断する。ここに、暗証照合命令データは、暗証照合機能コード、インデックス指定情報、および暗証番号情報（暗証番号レンジと暗証番号とからなる）によって構成されている。上記判断の結果、暗証照合命令データでなければ、制御素子15は、命令データ中の機能コードを解釈し、対応する処理を実行した後、その処理結果に対する応答データを出力し、命令データ待ち状態に戻る。

上記命令データの判断の結果、暗証照合命令データであった場合、制御素子15は、命令データ中のインデックス指定情報と一致するインデックスをデータメモリ16内の暗証情報テーブル162のインデックス部から検索する。この検索の結果、見付からなければ、制御素子15は、実行不可を意味する応答データを出力し、命令データ待ち状態に戻る。上記検索の結果、見付かった

する応答データを出力し、命令データ待ち状態に戻る。

さて、暗証番号の照合処理では、入力された命令データ中の暗証番号情報と指定された暗証番号とを比較照合する。この比較照合の結果、もし両者が一致していれば、制御素子15は、第1および第2のエラーカウンタを「00」とした後、インデックスに対応する暗証照合状態エリアを参照し、そのエリアの内容を読出すことにより、対応する照合状態ビットを「1」にし、照合完了を意味する応答データを出力し、命令データ待ち状態に戻る。

上記暗証番号の比較照合の結果、もし両者が一致していなければ、制御素子15は、インデックスに対応するエラーリミットエリアを参照し、そのエリアの内容を読出すことにより、下位4ビットの値（第2のエラーカウンタのリミット値）が「0」となっているか否かを判断する。この判断の結果、もし「0」となっていれば、制御素子15は、インデックスに対応する暗証照合状態エ

リアを参照し、そのエリアの内容を読出すことにより、対応する照合状態ビットを「0」にし、暗証番号不一致を意味する応答データを出力し、命令データ待ち状態に戻る。

上記エラーリミットエリアの下位4ビットの値の判断の結果、もし「0」となっていなければ、制御素子15は、エラーリミットエリアの上位4ビットの値(第1のエラーカウンタのリミット値)と第1のエラーカウンタの値とを比較照合する。この比較照合の結果、もし前者が後者よりも大きければ、制御素子15は、対応する第1のエラーカウンタの値を1つ増加する。そして、制御素子15は、インデックスに対応する暗証照合状態エリアを参照し、そのエリアの内容を読出すことにより、対応する照合状態ビットを「0」にし、暗証番号不一致を意味する応答データを出力し、命令データ待ち状態に戻る。

上記エラーリミットエリアの上位4ビットの値と第1のエラーカウンタの値との比較照合の結果、もし前者が後者よりも大きくなければ、制御素子

15は、インデックスに対応する第2のエラーカウンタエリアを参照し、そのエリアの内容を読出すことにより、第2のエラーカウンタの値と対応するリミット値(下位4ビットの値)とを比較照合する。この比較照合の結果、もし前者よりも後者の方が大きければ、制御素子15は、対応する第2のエラーカウンタの値を1つ増加する。そして、制御素子15は、インデックスに対応する暗証照合状態エリアを参照し、そのエリアの内容を読出すことにより、対応する照合状態ビットを「0」にし、暗証番号不一致を意味する応答データを出力し、命令データ待ち状態に戻る。

上記第2のエラーカウンタの値と対応するリミット値との比較照合の結果、もし前者よりも後者の方が大きくなければ、制御素子15は、インデックスに対応する暗証照合状態エリアを参照し、そのエリアの内容を読出すことにより、対応する照合状態ビットを「0」にし、暗証番号使用不可を意味する応答データを出力し、命令データ待ち状態に戻る。

なお、第7図で示すように、エラーカウンタエリアのエリア番号「12」および「13」は、インデックス「32」と「33」および「34」と「35」にそれぞれ対応している。これは、照合命令対象としてインデックス「32」に対応する暗証番号としても、また「33」に対応する暗証番号としても同一のエラーカウンタを使用することになる。また、インデックス「34」と「35」も同様な関係にある。さらに、特にインデックス「34」と「35」については、エラーリミット値も共有(エリア番号として「24」を共通に使用)している。これにより、たとえばインデックス「34」を使用した暗証番号の照合において、第2のエラーカウンタがリミット値に達してしまうと、同時にインデックス「35」を使用した暗証番号の照合も行えなくなる。

また、インデックス「32」と「33」に対応する暗証照合状態エリアのエリア番号も同一の「42」というエリア番号を示している。したがって、どちらを用いて照合を行なっても照合状態

フラグは第10図において1ビット目が「1」となる。

次に、トランザクションデータの書込み動作について第15図に示すフローチャートを参照して説明する。先の第1図において、入力された命令データが暗証照合命令データでなければ、制御素子15は、次に入力された命令データが第16図に示すようなフォーマットを持つトランザクションデータ書込み命令データか否かを判断する。ここに、トランザクションデータ書込み命令データは、トランザクションデータ書込み機能コード、エリア指定情報、および書込みデータによって構成されている。上記判断の結果、トランザクションデータ書込み命令データでなければ、制御素子15は、命令データ中の機能コードを解釈し、対応する処理を実行した後、その処理結果に対する応答データを出力し、命令データ待ち状態に戻る。

上記命令データの判断の結果、トランザクションデータ書込み命令データであった場合、制御素子15は、命令データ中のエリア指定情報と一致

するエリア番号をデータメモリ16内のトランザクションデータエリア定義テーブル165から検索する。この検索の結果、見付からなければ、制御素子15は、エリア未定義を意味する応答データを出力し、命令データ待ち状態に戻る。

上記エリア番号の検索の結果、見付かったならば、制御素子15は、そのエリア番号に対応するアクセス条件情報を参照し、そのアクセス条件情報の示す照合状態ビットが「1」になっているか否かを判断する。この判断の結果、もし「0」であれば、制御素子15は、アクセス不可を意味する応答データを出力し、命令データ待ち状態に戻る。上記判断の結果、もし「1」であれば、制御素子15は、トランザクションデータの書き込み処理を行ない、その処理結果に対応する応答データを出力し、命令データ待ち状態に戻る。

たとえば、第5図を参照すると、エリア番号「80」に対してはアクセス条件情報は「04」となっているので、照合状態ビットの2ビット目が「1」となっていれば、トランザクションデー

タの書き込みは可能である。したがって、インデックス「34」を用いた暗証番号の照合が正常に終了すれば、データエリア163内のエリア「80」にデータ書き込みが行なえることになる。また、エリア番号「81」は照合状態ビットの1ビット目が関係しているため、インデックス「32」または「33」を用いた暗証番号の照合が正常に終了すれば、データエリア163内のエリア「81」にデータ書き込みが行なえることになる。

このように、暗証番号の照合不一致時に参照する累積上限値(リミット値)を複数登録しておき、本ICカード内で定められた対応関係に基づき累積上限値を選択することにより、参照する累積上限値が複数の暗証番号に対して共通に使用されなくなり、暗証番号自身のセキュリティレベルの格差を確立できる。これにより、ICカードシステムのセキュリティ性確立方法が多様化する。

なお、前記実施例では、携帯可能電子装置としてICカードを例示したが、本発明はカード状のものに限定されるものではなく、たとえばブロッ

ク状あるいは棒状のものでもよい。また、携帯可能電子装置のハード構成も、その要旨を逸脱しない範囲で種々変形可能である。

【発明の効果】

以上詳述したように本発明によれば、暗証番号の照合不一致時に参照する累積上限値が複数の暗証番号に対して共通に使用されなくなり、暗証番号自身のセキュリティレベルの格差を確立できる携帯可能電子装置を提供できる。

4. 図面の簡単な説明

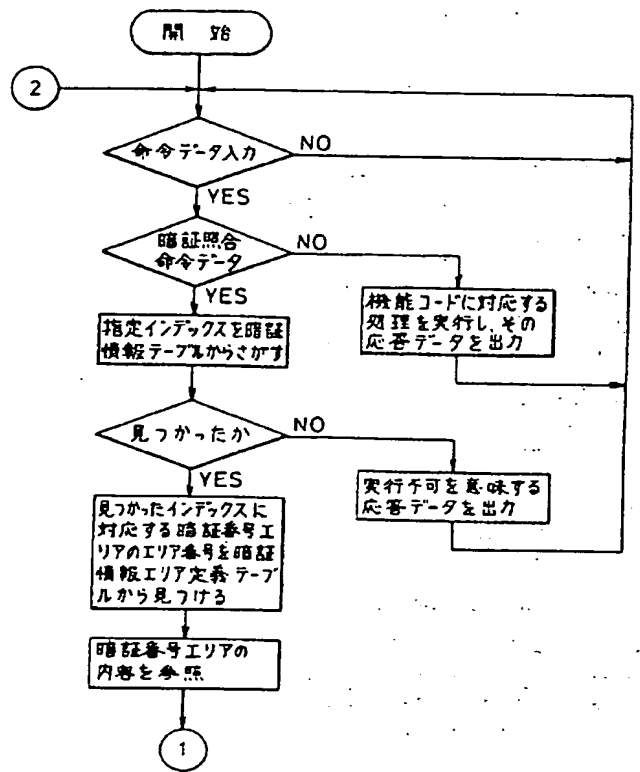
図は本発明の一実施例を説明するためのもので、第1図は暗証番号の照合動作を説明するフローチャート、第2図は暗証照合命令データのフォーマット例を示す図、第3図はデータメモリのフォーマット例を示す図、第4図は暗証情報エリア定義テーブルの具体例を示す図、第5図はトランザクションデータエリア定義テーブルの具体例を示す図、第6図はデータエリア内の格納データの具体例を示す図、第7図は暗証情報テーブルの具体例を示す図、第8図は第1のエラーカウンタエリア

を示す図、第9図はエラーカウンタエリアに格納されているリミット値のフォーマット例を示す図、第10図は照合状態ビットのフォーマット例を示す図、第11図はカードリーダー・ライタの動作を説明するフローチャート、第12図はICカードに入力される命令データのフォーマット例を示す図、第13図はICカードの動作を説明するフローチャート、第14図はICカードから出力される一般的な応答データのフォーマット例を示す図、第15図はトランザクションデータの書き込み動作を説明するフローチャート、第16図はトランザクションデータ書き込み命令データのフォーマット例を示す図、第17図はICカードの構成を示すブロック図、第18図はICカードの機能ブロックを示す図、第19図はカードリーダー・ライタの構成を示すブロック図、第20図は端末装置の構成を示すブロック図である。

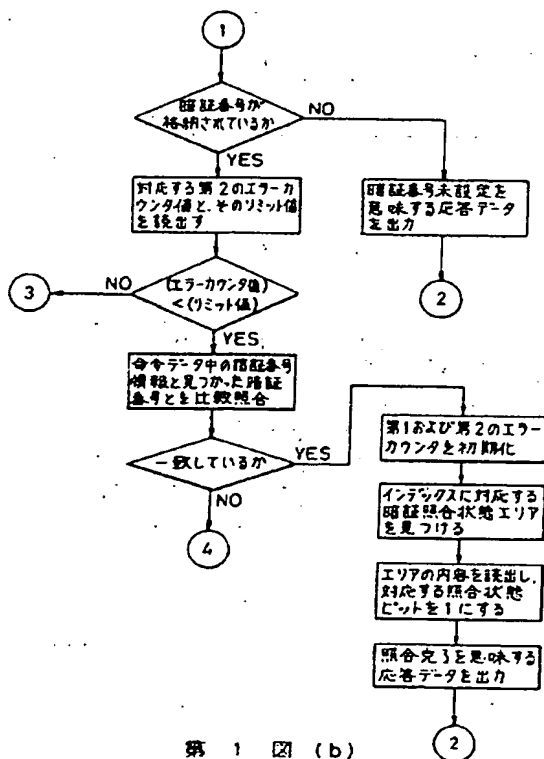
1…ICカード(携帯可能電子装置)、15…制御素子(制御部)、16…データメモリ(メモリ部)、17…プログラムメモリ、161…エリ

ア定義テーブル、162…暗証情報テーブル、
163…データエリア、164…暗証情報エリア
定義テーブル、165…トランザクションデータ
エリア定義テーブル。

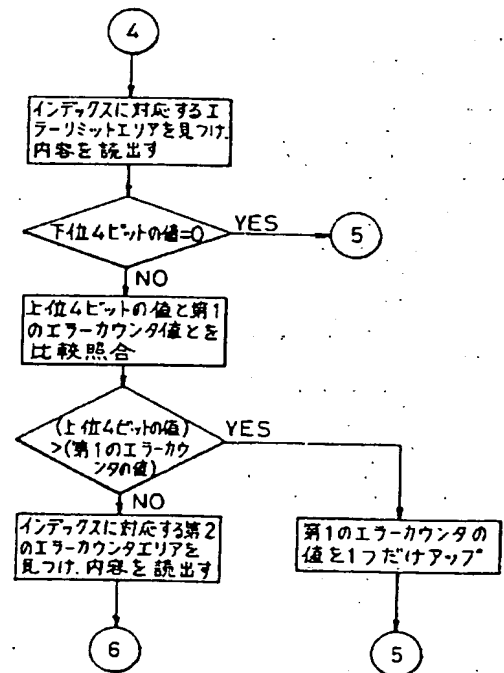
出願人代理人 弁理士 鈴江武彦



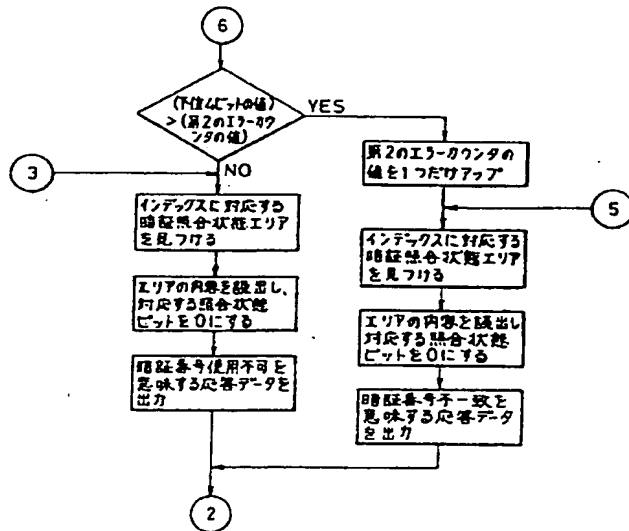
第 1 図 (a)



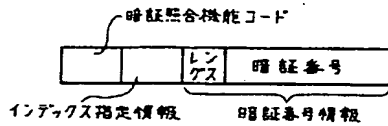
第 1 図 (b)



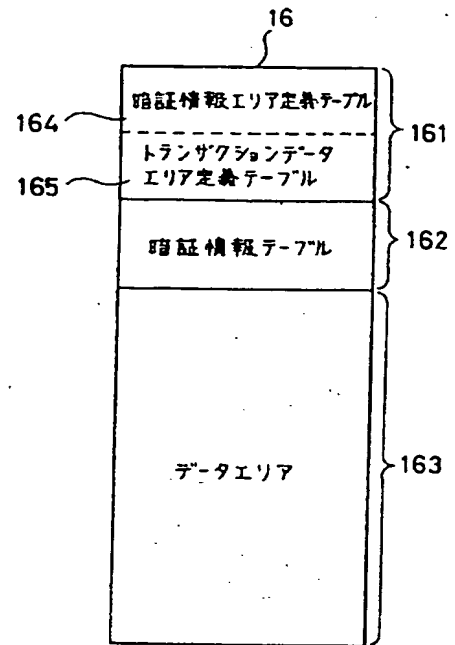
第 1 図 (c)



第 1 図 (d)



第 2 図



第 3 図

エリア番号	エリア先頭アドレス	エリアサイズ
01	TA01	10
02	TA02	10
03	TA03	10
04	TA04	5
05	TA05	5
11	TA11	1
12	TA12	1
13	TA13	1
21	TA21	1
22	TA22	1
23	TA23	1
24	TA24	1
41	TA41	1
42	TA42	1
43	TA43	1
44	TA44	1

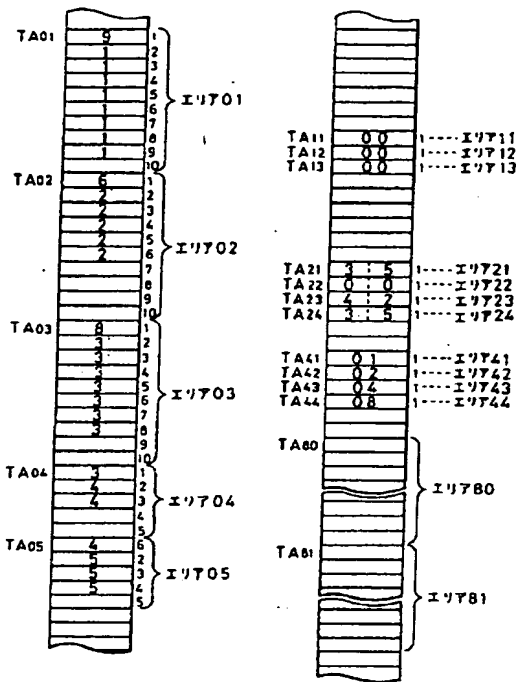
第 4 図

エリア番号	エリア先頭アドレス	エリアサイズ	アクセス条件情報
80	TA80	S80	04
81	TA81	S81	02

第 5 図

インデックス部	暗証番号エリアのエリア番号部	エラーカウンタエリアのエリア番号部	エラーリミットエリアのエリア番号部	暗証照合状態エリアのエリア番号部
31	01	11	21	41
32	02	12	22	42
33	03	12	23	42
34	04	13	24	43
35	05	13	24	44

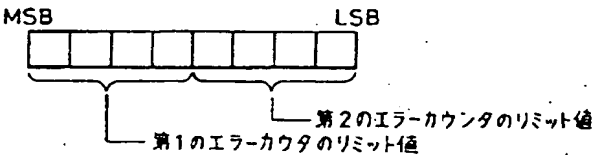
第 7 図



第 6 図

0 0	----- エリア11に対応
0 0	----- エリア12に対応
0 0	----- エリア13に対応

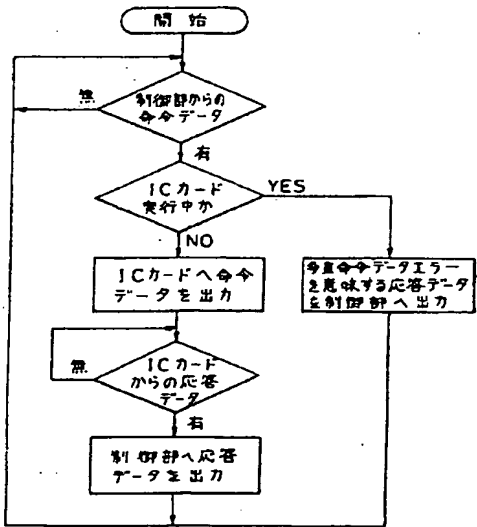
第 8 図



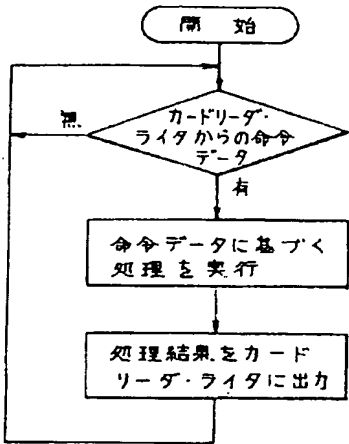
第 9 図

7	6	5	4	3	2	1	0
0	0	0	0	0	0	0	0

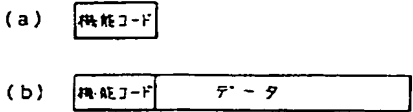
第 10 図



第 11 図



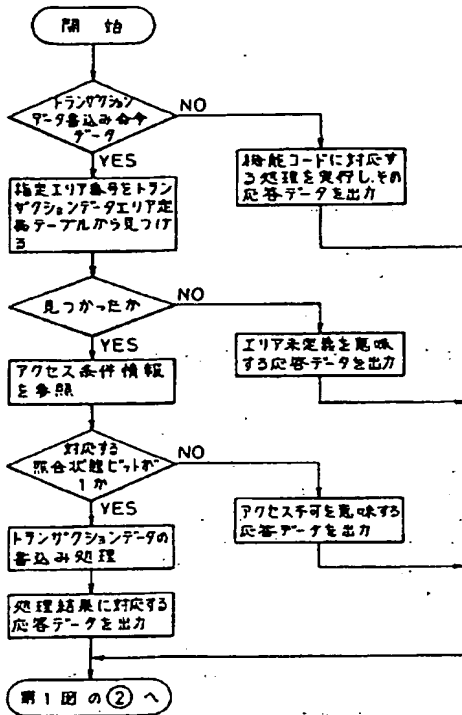
第 13 図



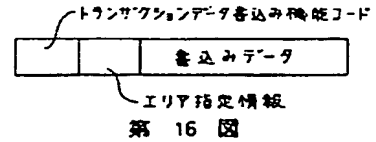
第 12 図

入力された命令データに含まれる機能コード	処理結果を示す情報
----------------------	-----------

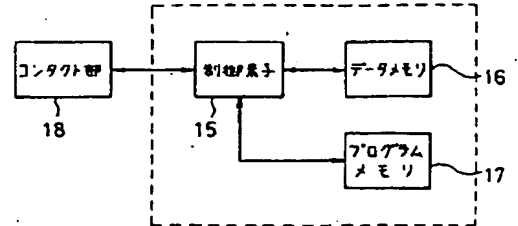
第 14 図



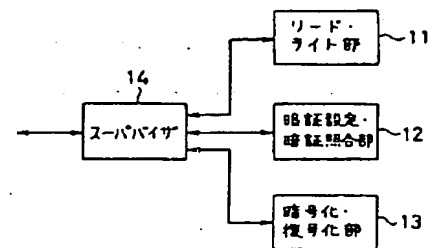
第 15 図



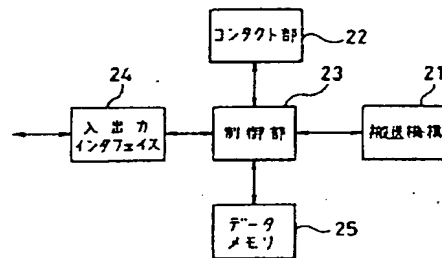
第 16 図



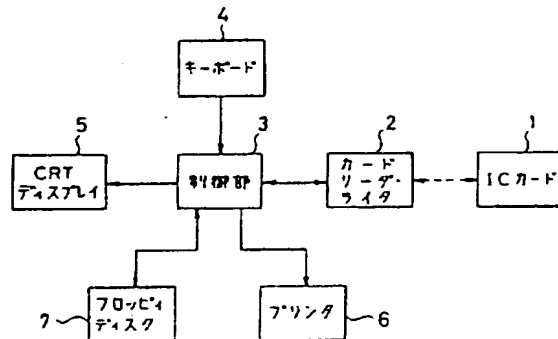
第 17 図



第 18 図



第 19 図



第 20 図